SYSTEM AND METHOD FOR DYNAMICALLY DETECTING COMPUTER VIRUSES THROUGH ASSOCIATIVE BEHAVIORAL ANALYSIS OF RUNTIME STATE

Abstract

A system and a method for dynamically detecting computer viruses through associative behavioral analysis of runtime state are described. A group of monitored events is defined. Each monitored event includes a set of one or more actions defined within an object. Each action is performed by one or more applications executing within a defined computing environment. The runtime state within the defined computing environment is continuously monitored for an occurrence of any one of the monitored events in the group. The sequence of the execution of the monitored events is tracked for each of the applications. Each occurrence of a specific event sequence characteristic of computer virus behavior and the application that performed the specific event sequence, are identified. A histogram describing the specific event sequence occurrence for each of the applications is created. Repetitions of the histogram associated with at least one object are identified.